

REMARKS

Status of Claims

Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 9-14, 17-23 and 33-35 are presently pending. Claims 9, 13, 17, 22 and 33-35 have been amended. No claims have been added, withdrawn or canceled. Claims 1, 22 and 33-35 are independent.

Statement of Substance of Interview

The Examiner graciously talked with me, the undersigned representative for the Applicant, on February 17, 2009. Applicant greatly appreciates the Examiner's willingness to talk. Such open communication is invaluable to both of us in our common goal of an expedited prosecution of this patent application.

During the interview, proposed amendments for overcoming the rejections of the claims under 35 USC §112 were discussed. The Examiner tentatively agreed that the proposed amendments would overcome the rejection, but indicated that she would need to examine the amendments more carefully upon receiving the formal response before making a final determination as to whether the amendments would overcome the rejections under 35 USC §112.

Also during the interview, I discussed how the claims differed from the cited references, and particularly Botz. I understood the Examiner to be receptive to the proposals, specifically the clarification regarding that the local machine is a single machine having a plurality of coexisting credential provider modules, each for logging a user on with the native operating system with one of a plurality of

different input devices. However, the Examiner indicated that she would need to review the cited art more carefully and/or do another search upon receiving the proposed amendments be presented in a formal response.

Applicant herein amends the claims in the manner discussed during the interview. Accordingly, Applicant submits that the pending claims are allowable over the cited art of record for at least the reasons discussed during the interview.

Formal Request for an Interview

If the Examiner's reply to this communication is anything other than allowance of all pending claims, and the only issues that remain are minor or formal matters, then I formally request an interview with the Examiner. I encourage the Examiner to call me, the undersigned representative for the Applicant, so that we can talk about this matter so as to resolve any outstanding issues quickly and efficiently over the phone.

Claim Amendments

Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claims 9, 13, 17, 22 and 33-35 herein. Applicant amends claims to overcome the rejections under 35 USC §112. Such amendments are made to expedite prosecution, and should not be construed as further limiting the claimed invention in response to the cited references.

SUBSTANTIVE MATTERS

Claim Rejections under § 112, Second Paragraph

Claims 9-14, 17-23 and 33-35 are rejected under 35 U.S.C. § 112, second paragraph. Applicant respectfully traverses this rejection. Furthermore, in light of the amendments presented herein, Applicant submits that these rejections are moot. Accordingly, Applicant asks the Examiner to withdraw these rejections.

Claim Rejections under § 103

The Examiner rejects claims 9-14, 17-23 and 33-35 under § 103. For the reasons set forth below, the Examiner has not made a *prima facie* case showing that the rejected claims are obvious. Accordingly, Applicant respectfully requests that the § 103 rejections be withdrawn and the case be passed along to issuance.

The Examiner's rejections are based upon the following references alone or in combination:

- **Botz:** *Botz, et al.*, US Patent Application Publication No. 2003/0177388 (published March 15, 2002);
- **Kao:** *Kao, et al.*, US Patent No. 6,651,168 (issued January 29, 1999);
- **Axel:** *Axel, et al.*, US Patent Application Publication No. 2004/0139355 (published November 7, 2002); and
- **Wen:** *Wen, et al.*, US Patent Application Publication No. 2003/0046392 (published March 6, 2003).

Overview of the Application

The Application describes a technology for logging a user on to a local machine using one or more credentials that are translated with one of a plurality of different credential provider modules initialized with a logon user interface. Each credential provider module translates a corresponding different type of credential into a common credential protocol. The translated credential is communicated through a logon UI module to an operating system (OS) of a local machine. An OS logon module is called by the logon UI module to authenticate the translated credential against a credential database. A user identified by the translated credential is logged on to access the local machine when the authentication is successful

Cited References

The Examiner cites Botz as the primary reference in the anticipation- and/or obviousness-based rejections. The Examiner cites Kao and Axel as secondary references in the obviousness-based rejections.

Botz

Botz describes a technology for authenticated identity translation based on a trust relationship between multiple user identification and authentication services resident on different computing units of a multiple computing unit environment. The technology includes recording user identification and authentication events occurring within the trusted domain, and making this

information available to other computing units within the domain by generating tokens representative of the identification and authentication events. A token is forwarded with a request to one or more computing units of the domain, which in turn provide the token to a domain controller to translate user identities between respective computing units.

Kao

Kao describes a technology for an authentication framework subsystem that enables a computer system to authenticate a user with a selected one of a plurality of authentication processes. Each of the authentication processes has a distinct sequence of steps and a unique input/output (I/O) interface for exchanging authentication information with the computer system. The invention includes an authentication framework in the computer system. An application program interface in the authentication framework provides an interface to an I/O component, such as a graphical user interface (GUI), of the computer system. A plurality of authentication modules interface with the framework. Each module has a conversation function driver defining a programmed sequence of steps to authenticate a user with a distinct authentication process.

Axel

Axel includes a method of accessing a plurality of network elements with at least one network element management program running on at least one element manager. The method comprises the steps of capturing a username and a password within the network element management program and submitting

the captured username and password to each of the plurality of network elements so as to effect administrative address privileges for each of said plurality of network elements without re-capturing said username and said password. The purpose of the method is to capture the username and password of the user in order to log the user into individual network elements without having to reenter his username and password.

Wen

Wen describes a technology for an automatic network connecting system that includes a database, a data managing module, a user interface module and a responding module. The database stores user private data and network connection public data. The data managing module accesses the user private data and the network connection public data stored in the database. The user interface module provides at least one prompt to a user, so that the user can input a network service request according to the prompt in one touch. The responding module receives the network service request and accessing the user private data and the network connection public data stored in the database through the data managing module according to the network service request to complete the network service requested by the user automatically.

Obviousness Rejections

Lack of *Prima Facie* Case of Obviousness (MPEP § 2142)

Applicant disagrees with the Examiner's obviousness rejections. Arguments presented herein point to various aspects of the record to demonstrate that all of the criteria set forth for making a *prima facie* case have not been met.

Based upon Botz

The Examiner rejects claims 9-11, 13-14, 17-19, 21-22 and 33 under 35 U.S.C. § 103(a) as being unpatentable over Botz in view of Kao. Applicant respectfully traverses the rejection of these claims and asks the Examiner to withdraw the rejection of these claims.

Independent Claims 9, 17 and 22

Applicant submits that the combination of Botz with Kao does not teach or suggest at least the following elements as recited in independent claim 9 (with emphasis added):

...initializing, by a native operating system (OS) on a local machine, a logon user interface (UI);

initializing, with the logon UI on the single local machine, a plurality of different coexisting credential provider modules, each for translating respectively

different types of credentials into a common credential protocol, the common credential protocol being compatible with the native OS of the local machine, each said credential provider module logging a user on with the native OS on the local machine via the logon UI to access the local machine using one of a plurality of corresponding different input devices in communication with the local machine;

receiving a first said credential from the user at a first one of said input devices in communication with the local machine;

translating the first credential with a first one of said credential provider modules corresponding to the first input device that is in communication with the local machine;

communicating the translated first credential having the common credential protocol through a credential provider Application Program Interface (API) to the logon UI of the native OS, wherein the credential provider API is configured to interface with each of the plurality of different coexisting credential provider modules;

passing the translated first credential having the common credential protocol to an OS logon module of the native OS from the logon UI;

calling the OS logon module for the native OS to authenticate the translated credential having the common credential protocol against a credential database; and

logging the user on with the native OS to access the local machine when the authentication is successful.

In making the rejection of independent claim 9, the Office Action states on page 6 that paragraphs 0008 and 0010 of Botz teach initializing, with the logon UI on the single local machine, a plurality of different coexisting credential provider modules, each for translating respectively different types of credentials

into a common credential protocol, the common credential protocol being compatible with the native OS of the local machine. However, Applicant notes that paragraph 0008 of Botz reads as follows:

In an enhanced aspect, the domain further includes a logical domain controller function, and the translating includes using the token to translate using the domain controller the authenticated user identity to the local user identity, wherein the translating includes employing a global registry of the different user identities maintained by the domain controller to translate the authenticated user identity into the local user identity for the subsequent authentication unit.

Applicant further notes that paragraph 0010 of Botz reads as follows:

Aspects of the present invention advantageously support application run-time inter-operation between disparate security registry services which employ different forms of user identification and authentication. In accordance with the authenticated identity translation technique disclosed herein, a caller of the service does not have to know which target system or systems a further request will be forwarded to in a multi-system environment. Further, using the present technique, user passwords exist only inside the protection offered by the security registry whereby a user initially authenticates, thereby facilitating administration of the system. Employing identity translation tokens in accordance with an aspect of the technique further provides trace delegation that encompasses multiple disparate security user registries. In addition, using a domain controller function to record identification and authentication events inside a domain enables management of a security state for a transaction in transit (emphasis added).

Thus, neither of the recited paragraphs of Botz teach or suggest initializing, with the logon UI on a single local machine, a plurality of different coexisting credential provider modules, each for translating respectively different types of credentials into a common credential protocol, the common credential

protocol being compatible with the native OS of the local machine. Instead, Botz merely discusses that aspects of his invention support application run-time inter-operation between disparate security registry services which employ different forms of user identification and authentication. Thus, Botz does not teach or suggest a plurality of different coexisting credential provider modules initialized on a single local machine, each for translating respectively different types of credentials into a common credential protocol compatible with the operating system, as recited in Applicant's claim 1. Instead, as shown at FIG. 2, Botz uses only one local user registry 208 at an initial authentication server 202. Similarly, at FIG. 13, Botz shows three initial authentication servers 1406, 1408 and 1410, each used by a different user for authentication, and each having only one local user registry. Applicant has been unable to locate any portion of Botz that discusses more than one registry per server. Accordingly, Applicant respectfully submits that Botz does not teach or suggest initializing, with the logon UI on the single local machine, a plurality of different coexisting credential provider modules, each for translating respectively different types of credentials into a common credential protocol, the common credential protocol being compatible with the native OS of the local machine, as recited in Applicant's claim 1.

Furthermore, the Office Action states at Page 7, lines 8-9, that Botz does not explicitly disclose a plurality of different input devices. The Office Action further indicates at page 7 that Kao discloses a local machine in communication with a plurality of different input devices, citing FIG. 1A and col. 8, lines 22-26 and 38-48 of Kao. However, the recited portions of Kao also fail to teach or suggest initializing, with the logon UI on the local machine, a plurality of different

coexisting credential provider modules, each configured for translating respectively different types of credentials into a common credential protocol, the common credential protocol being compatible with the native OS of the local machine, each said credential provider module configured for logging a user on with the native OS on the local machine via the logon UI to access the local machine using one of a plurality of corresponding different input devices in communication with the local machine, as recited in Applicant's claim 9.

Instead, Kao is directed to an authentication framework 200 that teaches that external APIs 214, 214' and 214'' within the authentication framework are exposed to interfaces 202, 204 and 206, respectively, for all authentication related operations within the authentication framework 200 (col. 8, lines 22-32). Kao also teaches authentication modules 208, 210, 212, but these authentication modules do not meet the limitation of claim 9 for translating different credentials into a common credential protocol compatible with the native OS of the local machine for logging a user on with the native OS. Thus, instead of teaching Applicant's method in which a plurality of different credential provider modules are initialized with a single logon UI at the single local machine for translating different types of credentials to a common credential protocol, Kao teaches multiple interfaces 202, 204 and 206 that are initialized separately from each other, that communicate with APIs 214, 214' and 214''. Thus, Kao's interfaces 202, 204, and 206 and authentication modules 208, 210, 212 perform no translation function of translating different credential types to a common credential protocol, the common credential protocol being compatible with the

native OS of the local machine, unlike the plurality of different coexisting credential provider modules initialized with the logon UI of Applicant's claim 9.

In view of the arguments set forth above, Applicant respectfully submits that neither Botz, nor Kao teaches or suggests initializing, with the logon UI on the single local machine, a plurality of different coexisting credential provider modules, each for translating respectively different types of credentials into a common credential protocol, the common credential protocol being compatible with the native OS of the local machine, each said credential provider module logging a user on with the native OS on the local machine via the logon UI to access the local machine using one of a plurality of corresponding different input devices in communication with the local machine. Consequently, as neither of these references teaches or suggests this feature of Applicant's invention, the combination thereof also cannot teach or suggest this feature.

Axel and Wen are cited as being relevant to the subject matter of claims 12, 20 and 23, and 13, 34 and 35, respectively, and provide no teachings regarding the subject matter of claim 9 discussed above. Accordingly, Applicant respectfully submits that claim 9 is in condition for allowance, and asks the Examiner to withdraw the rejection of claim 9.

Independent claims 17 and 22 include limitations similar to those discussed above with respect to claim 9, are allowable under a similar rationale, and thus are also in condition for allowance.

Independent Claim 33

Independent claim 33 includes limitations similar to those discussed above with respect to claim 9, and is allowable under a similar rationale. In addition, claim 33 includes (with emphasis added):

...initializing, by a native operating system (OS) on the local machine, a logon user interface (UI);

initializing, with the logon UI on the single local machine, a plurality of different coexisting credential provider modules, each said credential provider module performing a translation of a respectively different type of credential received at one of a plurality of different types of input devices in communication with the local machine for translating the respectively different types of credentials into a common credential protocol, the common credential protocol being compatible with the native OS of the local machine, wherein each said credential provider module logs a user on with the native OS on the local machine via the logon UI to access the local machine using one of the plurality of corresponding different input devices in communication with the local machine;

receiving a first credential from the user at a first said input device in communication with the local machine;

receiving a second credential from the user at a second said input device in communication with the local machine;

translating the first credential into the common credential protocol using a first one of the credential provider modules corresponding to the first input device that is in communication with the local machine;

translating the second credential into the common credential protocol using a second one of the credential provider modules corresponding to the

second input device that is in communication with the local machine;

using a component of the OS to authenticate the translated first credential and second credential having the common credential protocol against a credential database; and

logging the user on with the OS to access the local machine when the authentication of both the first credential and the second credential is successful.

The Office Action asserts on Pages 18-19 that these limitations are taught by Botz at par. 0094 and par. 0099-0106, and by Kao at col. 9, line 66 through col. 10, line 10; col. 8 line 64-67, and col. 17, lines 23-26. However, Applicant respectfully asserts that none of the cited portions of Botz or Kao teach or suggest a method using a first credential translated by a first credential provider module and a second credential translated by a second credential provider module, that includes logging the user on with an OS on a local machine when the authentication of both the first credential and the second credential is successful. For example, the cited portion of Botz at par. 0094 teaches that the AIT domain server accesses policy information about both the request server and the initial authentication server. However, this is not the same as receiving a first credential from a user and a second credential from a user, translating these credentials to a common credential protocol using respective first and second credential provider modules, and logging the user on with the OS when authentication of both the first credential and the second credential is successful.

Similarly, Kao at col. 8, lines 64-67, only teaches that a smart card 222 is plugged into the smart card reader 220 and a user's DCE ID and password is

stored in the smart card. The user needs to be authenticated by the smart card and its smart card authentication module 210. Then, the authentication framework 200 can retrieve the user's DCE ID and password from the smart card and use them to sign the user on. Thus, this portion of Kao does not teach a first credential translated into the common credential protocol by a first credential provider module and a second credential translated into the common credential protocol by a second credential provider module, or logging the user on with the OS to access the local machine when the authentication of both the first credential and the second credential is successful, as recited in Applicant's claim 33. Accordingly, as neither Botz, nor Koa teaches or suggests this feature of Applicant's invention, the combination thereof also cannot teach or suggest this feature.

Axel is cited as being relevant to the subject matter of claims 12, 20 and 23, and provides no teachings regarding the subject matter of claim 33. Similarly, Wen is cited as being relevant to the subject matter of claims 13, 34 and 35, and also provides no teachings regarding the subject matter of claim 33. Thus, Applicant respectfully submits that claim 33 is allowable over the Botz, Kao, Alex and the other art of record, whether taken singly, or in combination.

Independent Claim 34

Independent claim 34 includes limitations similar to those discussed above with respect to claim 9, and is allowable under a similar rationale. In addition, claim 34 includes (with emphasis added):

...initializing, by a native operating system (OS) on the local machine, a logon user interface (UI);

initializing with the logon UI on the single local machine a plurality of different coexisting credential provider modules, each for translating respectively different types of credentials into a common credential protocol, the common credential protocol being compatible with the native OS of the local machine, each said credential provider module logging a user on with the native OS on the local machine via the logon UI to access the local machine using one of a plurality of corresponding different input devices in communication with the local machine;

initializing one or more pre-logon access provider (PLAP) modules at the local machine coexisting with said credential provider modules, each PLAP module operating with the OS of the local machine so that the user selects a logon connection type out of a plurality of logon connection types for establishing a network connection;

receiving a first said credential from the user at a first one of said input devices in communication with the local machine;

translating the first credential with a first one of said credential provider modules corresponding to the first input device that is in communication with the local machine;

establishing, by a selected one of said PLAP modules, a network connection from the local machine to a domain using the translated first credential;

communicating the translated first credential having the common credential protocol through a credential provider interface to the logon UI of the native OS, wherein the credential provider interface is configured to interface with each of the plurality of coexisting different said credential provider modules;

passing the translated first credential having the common credential protocol to a logon routine of the native OS from the logon UI;

authenticating the translated first credential against a credential database with the logon routine of the native OS; and

logging the user on to access the local machine with the native OS when the authentication is successful.

Thus, according to this aspect of Applicants invention, one or more pre-logon access provider (PLAP) modules are initialized at the local machine, coexisting with said credential provider modules, each PLAP module being interoperable with the OS of the local machine for enabling the user to select a logon connection type out of a plurality of logon connection types for establishing a network connection. The network connection is established by a selected one of said PLAP modules, from the local machine to a domain using the translated first credential.

The Office Action asserts that one or more pre-logon access provider (PLAP) modules are initialized at the local machine, coexisting with said credential provider modules is taught by Wen at par. 0032 and FIGS. 3a-3B. However, the recited portion of Wen is directed to a system that can complete network connection procedures automatically according to the user's selection by only one touch, including a dial-up procedure and a log-in procedure. For example, if the user wants to browse a web page of a web server when the computer is not connected with the Internet, the system can firstly establish a network connection with an ISP according to the data stored in the database automatically. After connecting to the Internet, the system then connects to the

web server to download the content of the web page the user requested (par. 0032).

On the other hand, Applicant's claim is directed to initializing one or more pre-logon access provider (PLAP) modules at the local machine, coexisting with said credential provider modules. Applicant respectfully asserts that neither the above-recited portion of Wen, nor any of the other art of record teaches or suggests this aspect of Applicant's invention.

Further, the Office Action asserts that Applicant's limitation of establishing, by a selected one of said PLAP modules, a network connection from the local machine to a domain using the translated first credential is taught by Botz at par. 0007; Koa at col. 8, lines 22-26 and col. 9, lines 30-34; and Wen at par. 0032 and FIGS. 3A-3B. However, Applicant respectfully notes that none of the recited portions of these references teach or suggest initializing one or more pre-logon access provider (PLAP) modules at the local machine coexisting with said credential provider modules, and then establishing, by a selected one of said PLAP modules, a network connection from the local machine to a domain using the translated first credential, as recited in Applicant's claim 34. Accordingly, Applicant respectfully submits that claim 34 is allowable over Botz, Kao, Alex, Wen and the other art of record, whether taken singly, or in combination.

Independent Claim 35

Independent claim 35 includes limitations similar to those discussed above with respect to claim 9, and is allowable under a similar rationale. In addition, claim 35 includes (with emphasis added):

...initializing, by a native operating system (OS) on the local machine, a logon user interface (UI);

initializing, with the logon UI on the single local machine, a plurality of different coexisting credential provider modules, each said credential provider module configured to perform a translation of a respectively different type of credential received at a different type of input device in communication with the local machine for translating the respectively different types of credentials into a common credential protocol, the common credential protocol being compatible with the native OS of the local machine, wherein each said credential provider module logs a user on with the native OS on the local machine via the logon UI to access the local machine using one of a plurality of available corresponding different input devices in communication with the local machine;

choosing, by a user, one or more of said plurality of different types of input devices for logging on from among the plurality of available different input devices;

receiving a first credential from the user via a chosen first one of said input devices in communication with the local machine;

translating the first credential into the common credential protocol compatible with the native OS of the local machine with a first one of said credential provider modules that corresponds to the chosen first input device;

communicating the translated first credential having the common credential protocol through a credential provider interface to the logon UI of the native OS, wherein the

credential provider interface is configured to interface with each of the plurality of coexisting different said credential provider modules;

passing the translated first credential having the common credential protocol to a logon routine of the native OS from the logon UI;

authenticating the translated first credential against a credential database with the logon routine of the native OS; and

logging the user on to access the local machine with the native OS when the authentication is successful..

Thus, according to this aspect of Applicants invention, the user chooses which input device to use to log on to the local machine from among a plurality of available input devices. A first credential from the user via a chosen first one of the input devices is received and translated into the common credential protocol compatible with the native OS of the local machine with a first one of the credential provider modules that corresponds to the chosen first input device. The Office Action asserts at page 30 that the limitation of choosing an input device to log on to the local machine is taught by Wen at par. 0032 and FIGS. 3A-3B. However, the recited portion of Wen is directed to logging onto an ISP and a web server, not a local machine, as recited in Applicant's claim 35. Botz, Koa, Alex and the other art of record fail to make up for this shortcoming in Wen. Accordingly, Applicant respectfully submits that claim 35 is allowable over Botz, Kao, Alex, Wen and the other art of record, whether taken singly, or in combination.

Dependent Claims

In addition to its own merits, each dependent claim is allowable for the same reasons that its base claim is allowable. Applicant requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action**. Please call or email me at your convenience.

Respectfully Submitted,

Lee & Hayes, PLLC
Representatives for Applicant

_____/Colin D. Barnitz/

Dated: February 17, 2009

Colin D. Barnitz (colin@leehayes.com; x5002)

Registration No. 35061

Emmanuel Rivera (emmanuel@leehayes.com; x5001)

Registration No. 45760

Customer No. **22801**

Telephone: (512) 505-8162

Facsimile: (509) 323-8979

www.leehayes.com